

UNITED STATES DISTRICT COURT

FILED

for the
Eastern District of North Carolina

OCT 19 2015

JULIE RICHARDS JOHNSTON, CLERK
US DISTRICT COURT, EDNC
BY 88 DEP CLKIn the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)205 Duxbury Drive, Raleigh, NC, 27607 and
the Person of Ameer Abu-Hammad

Case No.

5:15-mj-2097

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):
205 Duxbury Drive, Raleigh, NC, 27607 and the Person of Ameer Abu-Hammad (as stated in Attachment A incorporated herein)

located in the Eastern District of North Carolina, there is now concealed (identify the person or describe the property to be seized):

See Attachments A, B, and C incorporated herein

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

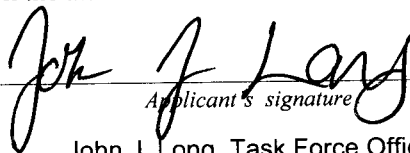
Code Section
18 U.S.C. § 2339B

Offense Description
Providing, attempting and conspiring to provide material support to a designated foreign terrorist organization

The application is based on these facts:

See Attached Affidavit herein.

- ☒ Continued on the attached sheet.
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



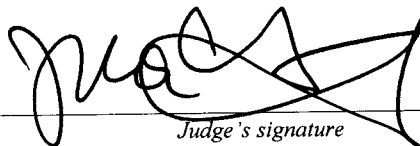
John J. Long, Task Force Officer

Printed name and title

Sworn to before me and signed in my presence.

Date:

19 October 2015

City and state: Raleigh, North Carolina


JAMES E. GATES, U.S. Magistrate Judge

Printed name and title

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, John J. Long, being duly sworn, depose and say:

1. I make this affidavit in support of an application for a search warrant for the residence located at 205 Duxbury Drive, Raleigh, NC, 27607 and other items to include but not limited to computer(s) and cellular telephones as described below. The residence can be described as a two story, brick front, single-family residence located in the Braeloch neighborhood. The aforementioned residence is where AMEER ABU-HAMMAD, the subject of this investigation resides. The items and information to be searched are described in the following paragraphs and in Attachment A.
2. I am employed as a Special Agent with the North Carolina State Bureau of Investigation (NCSBI), currently assigned as a Joint Terrorism Task Force Officer (TFO) with the Federal Bureau of Investigation (FBI). I have served in a law enforcement capacity since February 1998. Throughout my law enforcement career I have attended schools and training programs concerning the investigation of terrorism, financial crimes, sexual assaults, homicide investigation, drug investigation, and other violations of North Carolina and Federal Law. I have received specialized training through the North Carolina Justice Academy and have completed the Criminal Investigations Certificate Program. I also have an advanced law enforcement certificate through the criminal justice education and training standards commission of North Carolina. I have been involved in numerous criminal investigations in the past that have led to successful prosecutions.
3. The facts set forth in this affidavit are based on knowledge obtained through my participation in this investigation and information provided to me by other law enforcement officers involved in the investigation. This affidavit is being submitted for the sole purpose of establishing probable cause to support the requested search warrants. I have set forth only the facts necessary to support this request for search warrants for the facilities requested in Attachment A, and I have not included every fact known to me concerning this investigation.
4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 2339B, providing, attempting, and conspiring to provide material support to a designated foreign terrorist organization, have been committed by AMEER ABU-HAMMAD and that evidence, fruits and instrumentalities of the violations will be found within his residence, computer(s) and cellular telephones.

BACKGROUND REGARDING COMPUTERS, THE INTERNET, AND E-MAIL

5. The term "computer" as used herein is defined by Title 18, United States Code, Section 1030 (e) (1), and includes any electronic, magnetic, optical, electrochemical, or other high speed data processing device, to include cellular phones, also known as "smart phones," performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.



6. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience and knowledge, I know the following:
- a. The internet is a worldwide network of computer systems operated by governmental entities, corporations, and universities. In order to access the internet, an individual computer user must subscribe to an access provider, which operates a host computer system with direct access to the internet. The World Wide Web ("WWW") is a functionality of the internet which allows users of the internet to share information;
 - b. With a computer connected to the internet, an individual computer user can make electronic contact with millions of computers around the world. This connection can be made by any number of means, including modem, local area network, wireless, and numerous other methods; and
 - c. E-mail is a popular form of transmitting messages and/or files in an electronic environment between computer users. When an individual computer user sends e-mail, it is initiated at the user's computer, transmitted to the subscriber's mail server, and then transmitted to its final destination. A server is a computer that is attached to a dedicated network and serves many users. An e-mail server may allow users to post and read messages and to communicate via electronic means. Companies that provide e-mail services include, but are not limited to: Google Gmail, Yahoo!, Microsoft Hotmail, Microsoft Live, and other internet service provider specific accounts like AOL (America Online) or Time Warner Cable.
 - d. An Internet Protocol (IP) address is a numerical label assigned to a device or company by an Internet Service Provider (ISP) when that device connects to the internet. IP addresses are assigned to a user either anew at the time of connecting to the internet or permanently by fixed configuration. Permanent configuration is known as using a static IP address. In contrast, when the computer's IP address is assigned newly for each connection with the internet, this is known as a dynamic IP address. There are various ISPs available depending on where a user lives. These ISPs host a block of IP addresses that are distributed out to users when the users connect into the internet. ISPs maintain historical data on IP addresses used by their subscribers. These IP addresses, in combination with their date and time of connection with the internet, can then be traced by the ISP back to a specific subscriber.

FACEBOOK

7. Facebook owns and operates a free-access social networking website of the same name that can be accessed at <http://www.facebook.com>. Facebook allows its users to establish accounts with Facebook, and users can then use their accounts to share written news,



photographs, videos, and other information with other Facebook users, and sometimes with the general public. Facebook users can exchange private messages on Facebook with other users. These messages, which are similar to e-mail messages, are sent to the recipient's "Inbox" on Facebook, which also stores copies of messages sent by the recipient, as well as other information. Facebook users can also post comments on the Facebook profiles of other users or on their own profiles; such comments are typically associated with a specific posting or item on the profile. Facebook also retains Internet Protocol ("IP") logs for a given user ID or IP address.

PROBABLE CAUSE

SUBJECT PREMISES AND ITEMS

8. As set out in more detail below, the investigation has revealed that AMEER ABU-HAMMAD is a United States citizen, a resident of Raleigh, North Carolina, with an address of **205 Duxbury Drive, Raleigh, NC, 27607**, who, among other things, is attempting to provide and/or conspiring to provide material support to ISIS. During the investigation, law enforcement used multiple confidential human sources (CHSs) and an online covert employee (OCE) to gather information concerning ABU-HAMMAD through Facebook and other online communications platforms.
9. Facebook records display that the listed subscriber of Facebook account "ameer.abuhammad" is "Ameer Abu-Hammad." Many of these communications are provided below to support a probable cause showing that ABU-HAMMAD is involved in committing a violation of 18 U.S.C. Section 2339B.
10. Moreover, the evidence displays that there is probable cause that these communications were made using devices capable of accessing the internet and sending and receiving such communications. According to Facebook records, the account "ameer.abuhammad" has an identified Internet Protocol (IP) address that belongs to Time Warner Cable. Records from Time Warner Cable in turn confirm that the aforesaid IP address was being utilized from the residence located at **205 Duxbury Dr, Raleigh, North Carolina 27607**. The investigation has confirmed through publicly available records and physical surveillance that HAMMAD resides at this address with his parents and two younger brothers.
11. The internet service provided by Time Warner Cable to ABU-HAMMAD's home is capable of being accessed by one of two means. Commonly, a wi-fi router is connected to the service, which thus enables any wi-fi capable device within range of connecting to the internet service. Subsequent investigation, such as physical surveillance, has confirmed that ABU-HAMMAD in fact resides at this residence. The investigation has additionally determined that ABU-HAMMAD uses a smart phone (a Samsung Galaxy Smartphone) to connect to the internet via wi-fi. This has been confirmed through surveillance and statements by ABU-HAMMAD to a confidential human source (CHS).

12. The investigation has additionally discovered that ABU-HAMMAD has access to other computer media from his home because he has created digital documents sent from that residence that require capabilities beyond that of a smartphone.

ISIL

13. On October 15, 2004, the United States Secretary of State designated al-Qa'ida in Iraq, then known as Jam'at al Tawhid wa'al-Jihad, as a Foreign Terrorist Organization ("FTO") under Section 219 of the Immigration and Nationality Act and as a Specially Designated Global Terrorist under section 1(b) of Executive Order 13224. On May 15, 2014, the Secretary of State amended the designation of al-Qa'ida in Iraq as a FTO under Section 219 of the Immigration and Nationality Act and as a Specially Designated Global Terrorist entity under section 1(b) of Executive Order 13224 to add the alias Islamic State of Iraq and the Levant ("ISIL") as its primary name. The Secretary also added the following aliases to the ISIL listing: the Islamic State of Iraq and al-Sham ("ISIS"), the Islamic State of Iraq and Syria ("ISIS"), ad-Dawla al-Islamiyya fi al-'Iraq wa-sh-Sham, Daesh, Dawla al Islamiya, and Al-Furqan Establishment for Media Production. Although the group has never called itself "Al-Qaeda in Iraq," this name has frequently been used to describe it. In an audio recording publicly released on June 29, 2014, ISIS announced a formal change of ISIS's name to Islamic State ("IS"). On or about September 21, 2014, ISIL spokesperson Abu Muhammad al-Adnani called for attacks against citizens – civilian or military – of the countries participating in the U.S. led coalition against ISIL. To date, ISIL remains a designated FTO.

AL-NUSRAH

14. On October 15, 2004, the United States Secretary of State designated al-Qa'ida in Iraq ("AQI"), then known as Jam'at al Tawhid wa'al-Jihad, as a Foreign Terrorist Organization ("FTO") under Section 219 of the Immigration and Nationality Act and as a Specially Designated Global Terrorist under section 1(b) of Executive Order 13224.
15. On December 11, 2012, the Secretary of State amended the designation of AQI to include the following aliases: al-Nusrah Front ("ANF"), Jabhat al-Nusrah, Jabhet al-Nusra, The Victory Front, and Al-Nusrah Front for the People of the Levant.
16. On May 15, 2014, the Secretary of State, in response to the evolving nature of the relationships between ANF and AQI, amended the FTO designation of AQI to remove all aliases associated with al-Nusrah Front. Separately, the Secretary of State then designated al-Nusrah Front, also known as Jabhat al-Nusrah, also known as Jabhet al-Nusra, also known as The Victory Front, also known as Al-Nusrah Front for the People of the Levant, also known as Al-Nusrah Front in Lebanon, also known as Support Front for the People of the Levant, and also known as Jabaht al-Nusra li-Ahl al-Sham min Mujahedi al-Sham fi Sahat al-Jihad, as a Foreign Terrorist Organization ("FTO") under Section 219 of the Immigration and Nationality Act and as a Specially Designated Global Terrorist entity under section 1(b) of Executive Order 13224. To date, ANF remains a designated FTO.

SUBJECT COMMUNICATIONS

17. The CHSs used a Facebook page which ostensibly promoted the ideology of Islamic extremism. Some examples of the communications through Facebook between the CHSs, OCE, and ABU-HAMMAD are set out below.
18. An open-source review of ABU-HAMMAD's Facebook account revealed that on August 27, 2014, ABU-HAMMAD posted the following: "I dont need to make new friends in college right now, completing my mission is the most important thing."¹ Attached to this post was an Emoticon² of "feeling motivated."
19. On or about September 2, 2014, ABU-HAMMAD made the following Facebook comments regarding the beheading of journalist, Steven Sotloff: "You do know they're executing journalists so they can stop the US airstrikes and arming kurds? & they claim that those journalists are spreading lies against Islamic State. But what do i know? Im only a Jabhat al Nusra fan."
20. On or about September 21, 2014, ABU-HAMMAD made a post to his Facebook account expressing his frustration with both college and the pressure that his parents are placing on him to study. At the end of this post ABU-HAMMAD wrote: "...I will have no problem with quitting my college & recklessly switching to my extremist side. I'm an Islamic knight not a fucking nerd!!" This prompted another Facebook user to ask what is stopping him, to which he replied "I'm just waiting for my unexpected moment no matter how long it takes."³
21. On or about September 20, 2014, ABU-HAMMAD engaged in a Facebook conversation with a confidential human source (CHS# 1) in which CHS #1 asked ABU-HAMMAD, "I mean, what are your dreams?" ABU-HAMMAD responded, "Ohh, I want to help the oppressed people & children in gazaTo defend them with my lifeEven if it gets me killed." Later CHS #1 asked, "How can you do that though?...how can you defend them from here" ABU-HAMMAD answered, "No I meant travel to gaza lol, instead being like those activist that chant "free gaza" yet they do nothing." Your affiant is aware that often times US based individuals who wish to engage in jihad overseas use humanitarian efforts as their reasoning for travel in order to avoid suspicion from law enforcement.
22. On or about September 24, 2014, an open-source review of ABU-HAMMAD's Facebook account revealed that he made the following posting: "Yo Obama, if you think it's cool to bomb & massacre us Muslims with your airstrikes, you might as well kill me along with

¹ Errors original to quoted materials have been maintained throughout.

² Your affiant is aware that the term "Emoticon" is a pictorial representation of a facial expression which is commonly used on social media sites to express how a person is feeling.

³ At present, ABU-HAMMAD is enrolled as a full-time student at Wake Technical Community College in NC.

them. Cause I'll never turn a blind eye & watch you get away with it, you hypocritical ape bastard." Your affiant assesses that this comment was in reference to the American airstrikes against ISIS in al-Raqqa which occurred on or around September 23, 2014.

23. According to further open-source reviews, on or about September 25, 2014, ABU-HAMMAD wrote: "The best way to defeat your enemy is to learn about them, know their weaknesses & then prepare your attack."
24. On or about September 29, 2014, ABU-HAMMAD had a Facebook conversation with an individual whom he believed to be located in Syria and to be an active member of ISIS. This conversation was initiated with ABU-HAMMAD posting, "I desire death as much as you desire life," on his Facebook page. The aforesaid individual responded to ABU-HAMMAD by saying "comen to here" (referring to Syria). ABU-HAMMAD answered back saying, "Soon.....inshallah."⁴
25. On or about October 15, 2014, ABU-HAMMAD posted on his Facebook account, "Life is bullshit, education is pointless bullshit, having a job is pointless bullshit, love is pointless bullshit, this world is full of bullshits...The only thing I desire is to die as a shaheed/martyr."⁵ Approximately ninety minutes after posting this, ABU-HAMMAD edited the post by removing the portion "The only thing I desire is to die as a shaheed/martyr." Your affiant believes the editing demonstrates ABU-HAMMAD's increasing suspicion of potential monitoring of his account by the FBI and further reveals his true intentions.
26. In December of 2014, an open-source review of ABU-HAMMAD's online presence revealed an "Ask.fm" blog account which is facilitated by ABU-HAMMAD. "Ask.fm" is a question-answer blog whereby anonymous users post a question to a person's blog. The person being asked the question, in this case ABU-HAMMAD, receives electronic notice that a question has been asked and can then either decide to answer or delete the question. If answered, both the answer and the original question appear on the blog which is viewable to the public. In or around September of 2014, ABU-HAMMAD was asked: "What is happiness for you?" The answer provided by ABU-HAMMAD was: "Getting the hell out of this country forever."
27. On or about December 15, 2014, during a conversation with CHS#2, ABU-HAMMAD demonstrated a clear willingness to travel to the Middle-East to engage in violence. ABU-HAMMAD said he "would join the Palestinian resistance and fight Israel lol Cuz in my

⁴ Your affiant is aware that the Arabic term "inshallah" can be defined as meaning "If Allah wills it."

⁵ Your affiant is aware that the Arabic terms "shaheed/martyr" is used to honor a Muslim who has died fulfilling a religious commandment, especially those who die fighting jihad. Further, the Arabic term "jihad" has many meanings pertaining to a struggle (both internally and externally), but extremists use this term synonymously with fighting, war, and engaging in physical violence.

40's i wont have my parents with me in this world & maybe i would be on my own. When do you think is a good time to be a fighter?"⁶

28. On or about January 2, 2015, an open-source review of ABU-HAMMAD's Facebook account revealed that he changed the "cover photo"⁷ of his Facebook page. This new graphic shows what appears to be a bearded male fighter holding a firearm while donning a black headband and carrying a black flag. Both the flag and headband are items that are commonly attributed to the foreign terrorist organization ISIS (See the below image). Additionally, three days later on or about January 5, 2015, an open-source review of ABU-HAMMAD's Facebook account revealed that he replaced the aforementioned ISIS image with another cover photo. This second graphic appears to glorify the Mujahideen⁸. The cover photo reads "Mujahideen Never Dies" (see images below).



⁶ Your Affiant recognizes that ABU-HAMMAD often intermingles fighting for a Palestinian resistance against Israel (not necessarily a Designated Foreign Terrorist Organization (FTO)) with fighting for groups such as ISIS and Jabhat al-Nusrah (both of which are FTOs). See also image at para. 28. However, the fact that ABU-HAMMAD seems to place these on equal footing and that both are potential routes he will take does nothing to diminish the probable cause established by the facts within this affidavit that ABU-HAMMAD's electronics and residence will contain evidence of a violation of 18 U.S.C. §2339B.

⁷ A Facebook cover photo is an image that appears at the top of a user's Facebook page. A cover photo is an image that is larger than a user's profile picture and, similar to the profile picture, it is only changed by the user. Both the cover photo and profile picture are viewable to the public.

⁸ Your Affiant is aware that "Mujahideen" is an Arabic term used to describe Muslim guerrilla fighters such as those in Afghanistan, Iraq, and Syria.

29. On or about January 13, 2015, and in an apparent reference to the Charlie Hebdo terrorist attack in Paris, France⁹, ABU-HAMMAD posted the following comment on Facebook: "Muslims are one of the biggest idiots in this world....They're being slaughtered worldwide & beg for someone to save the Ummah¹⁰ (Muslim Creed), but when a group of "jihadists" decide to take a stand; Muslims apologize & unite with their killers without hesitation & then blame Israel for everything... #NotMyName #CharlieHebdo #BostonBomber #IslamIsPeace #ISIL..."
30. Additionally on or about February 4, 2015, ABU-HAMMAD made the following Facebook post regarding Moaz al-Kasasbeh, who was the captured Jordanian pilot that was reportedly burned alive in a cage by ISIS: "I wish I could post the pictures here, but you should see the burned children this pilot bombed and the limbs they've lost... this pilot is also a murderer."
31. On or about February 15, 2015, ABU-HAMMAD posted a video on his Google+ account titled: (ISIS Militants Beheading 21 Coptic Christians), to which ABU-HAMMAD commented, "According to ISIS, they are Christians of the church that tortured and killed Camilia and other girls for converting to Islam." The content of the video has been removed however the "shell" of the video and its hyperlink remain on his Google+ homepage. An open-source search of this video title results in numerous returns. While these results vary slightly in both length and quality, they all appear to be the same video which shows numerous individuals wearing orange jumpsuits being escorted along a shoreline by other men dressed all in black. Later in the video, the men who are wearing orange jumpsuits are all beheaded with fixed-blade knives. Having viewed this video, your affiant assesses that the video was likely removed by the original provider, YouTube, due to its extremely graphic content as well as its promotion of terrorist activity.
32. On or about February 16, 2015, ABU-HAMMAD posted the following comment on Facebook in response to ISIS reportedly publically releasing the aforementioned video: "Muslims should stop blaming Israel & the West that they're the ones funding ISIS. ISIS are a group of pissed off Muslims, whether you like it or not. & even if they are misguided or brutal, its haram¹¹ to ally yourself with the kuffar¹² against them."

⁹ Charlie Hebdo is a French satirical weekly magazine based out of Paris, France. On the morning of January 7th, 2015, the company was targeted by two gunmen who identified themselves as belonging to the Islamic terrorist group al-Qa'ida in the Arabian Peninsula (AQAP). The attack, which killed twelve people, is widely believed to be retaliation for the earlier publication of a cartoon drawing of the Prophet Muhammad. Any drawing or physical recreation of the Prophet Muhammad is strictly forbidden in the Islamic faith.

¹⁰ Your Affiant is aware that "Ummah" is an Arabic term used to describe the community of Islam and/or the worldwide Muslim community.

¹¹ Your Affiant is aware that the Arabic word "haram" is used to describe something that is illegal or prohibited within the Islamic faith.

¹² Your Affiant is aware that the Arabic word "kuffar" is most commonly used to describe a nonbeliever of Islam or a non-Muslim. It can also be interchanged with "infidel."

33. On or about February 16, 2015, ABU-HAMMAD posted a Facebook response to another Facebook user pertaining to a report that the uncle of Omar al-Baghdadi, who is assessed to be the leader of ISIS, was arrested in Iraq. This other user posted: "burn that idiot demoncults don't show mercy onthem" . ABU-HAMMAD responded with the following: "People like you show the evil disgusting side of israeli jews. Thank god hitler wiped 6 million of u guys."
34. On or about February 28, 2015, ABU-HAMMAD made the following post on Facebook, "I am as miserable as a lion in a cage forced to live his life acting in a circus."
35. On or about May 7, 2015, ABU-HAMMAD made the following post on Facebook in an apparent reference to ISIS executing more Christians in the Middle-East: "Muslims dont care when innocent Muslims are slaughtered everyday by the drones & bullets of the 'Crusaders'¹³ But Muslims are willing to shed a tear and unite with their enemies when Islamic extremists execute a few Christians...."
36. On or about May 13, 2015, in one of his most recent private posts, ABU-HAMMAD posted the following comment on Facebook; "Alhamdullilah¹⁴ the Al-Mighty, the Most Merciful Allah (swt)¹⁵ keeps guiding me to the right path as a righteous Tawheed¹⁶-believing Muslim while it still saddens me that a majority of young American Muslims here have gone astray, deceived by apostates, nationalism, & adultery."
37. On September 4, 2015, an open-sourced review of ABU-HAMMAD's Facebook account identified a YouTube account recently utilized by ABU-HAMMAD to post links to a "Nasheed" channel.¹⁷ Your affiant is aware that the Arabic term "Nasheed" refers to chants and generally describes a religious themed work of vocal music either sung a Capella or accompanied by percussion instruments. Your affiant is aware that Nasheed videos are commonly utilized by extremists to recruit, radicalize, and motivate individuals towards violent *jihad*. On this publicly accessible YouTube page, ABU-HAMMAD posted a link to

¹³ Your Affiant is aware that the word "Crusader" is often used to describe Christians, non-Muslims, and the Western powers in general.

¹⁴ Your Affiant is aware that the Arabic word "Alhamdulillah" means praise be to Allah and is a phrase said to give thanks to God.

¹⁵ Your Affiant is aware that when many Muslims write the Arabic word "Allah," they also follow it with the abbreviation "SWT." These letters stand for the Arabic words "Subhanahu Wa Ta'ala" which translated means "Glory to Him, the Exalted." Muslims commonly use these words to glorify God when mentioning his name.

¹⁶ Your Affiant is aware that the Arabic word "Taweed" is used to describe the "Oneness of Allah" meaning that Allah is one and unique.

¹⁷ YouTube is a video sharing website allowing users to upload, view, and share originally created videos or otherwise obtained video clips.

a video entitled "Jihad Nasheed." The video contains a Nasheed sung entirely in Arabic, advocating "*jihad*", and depicting an image of an assault rifle in the background.

INFORMATION TO BE SEARCHED AND ITEMS TO BE SEIZED

38. I anticipate that the execution of this search warrant for the residence described in Attachment A, will reveal computers, laptops and at least one smart phone (a Samsung Galaxy Smartphone), capable of being utilized by ABU-HAMMAD to access the internet and communicate on-line. Seizure of the aforementioned computer(s), laptops, cellular phones, as well as any other electronic devices capable of communication via the internet and potentially capable of containing records, documents, or other materials as described in affidavit will be necessary so that a comprehensive examination can be conducted. Your affiant recognizes that ABU-HAMMAD resides with his parents and younger brother; therefore, this search request is limited to the common areas of the residence accessible by ABU-HAMMAD (e.g., kitchen, living room, family room, etc.) and any personal space he may possess (e.g, his designated room and/or sleeping space); this is intended to specifically exclude such as areas his parent's and brothers' room(s) – presuming there is no indication that he has access to and uses any computer media in such areas or stores any personal property in such areas.
39. Similarly, extracting information from computers and cellular telephones requires law enforcement to seize the computers, cellular telephones, and related storage devices along with related peripherals and if necessary, search them later by a qualified person in a laboratory or other controlled environment. This is true because of the following:
 - a. The volume of the evidence. Computers and cellular telephones occasionally contain storage devices such as, hard disks, memory cards, and other related storage devices and can store the equivalent of hundreds of thousands of pages of information. Additionally, a person may try to conceal criminal evidence by storing it in random order with deceptive file names. This may require searching authorities to examine all the stored data to determine which particular files are evidence or instrumentalities of crime. This sorting process takes time, up to weeks or months, depending on the volume of data stored. It would also be impractical to attempt this type of data search on site.
 - b. Technical requirements. Searching computers and cellular phones and their storage systems for criminal evidence is a highly technical process requiring skill and a properly controlled environment. The vast array of technical hardware and software available requires computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer and cellular telephone and related storage systems is an exacting scientific procedure which is designated to protect the integrity of the evidence and to recover even "hidden", erased, compressed, password protected or encrypted files.

- c. The compatibility of peripheral devices and software. The peripheral devices which allow users to enter or retrieve data from the storage devices vary widely in their compatibility with other hardware and software. Many system storage devices require particular input/output devices in order to read the data on the system. It is important that the analyst be able to properly reconfigure the system as it now operates in order to accurately retrieve the evidence listed above.

CONCLUSION

40. Over the course of this investigation, ABU-HAMMAD has grown increasingly suspicious of potential FBI monitoring of his online activities. During the summer of 2014, ABU-HAMMAD routinely posted radical thoughts, pictures, and videos in a manner that was viewable to the public (open-source). Toward the latter part of 2014 ABU-HAMMAD suddenly changed his Facebook privacy settings in a way that made the majority of his postings and other material only viewable to a closed-network of friends. Your affiant assesses that this is consistent with extremists who either recognize the need or have been informed of the need to be "security conscious" because of their intent to unlawfully act on their radical beliefs.
41. The collective picture from ABU-HAMMAD's communications displays from his own words, that he is a "Jabhat al-Nusrah fan," he is willing to switch to his "extremist side" because he views himself as an "Islamic Knight," that he may travel at any "unexpected moment no matter how long it takes," that "the only thing" he desires is "to die as a shaheed/martyr," and he holds to the belief that that the U.S. is a crusader nation murdering Muslims and it would be improper for Muslims to fight against ISIS whose violence is justified. Moreover, ABU-HAMMAD informed a person he believed to be an ISIS fighter in Syria that, God willing, he would be coming "soon." In contrast to any indication that he has foregone these beliefs, he has recently posted propaganda advocating violent *jihād*. See *supra* (specifically paragraphs 19, 20, 24, 25, 28, 32, 35, 27).
42. Your affiant assesses that his only identified reservation is the fact that ABU-HAMMAD feels it would be "haram"¹⁸ if he were to travel to fight while his parents are still alive. Your Affiant however notes that the extremist ideology of groups such as ISIS and Jabhat al-Nusrah is one that both contemplates and propagates the typical jihadist principle that they are involved in a long-term conflict (often referred to as a "100 year war") and thus action may be held off until the most opportune and appropriate moment.
43. I believe that there is probable cause that evidence of violations of Title 18, United States Code, Section 2339B, will be found within the communication devices located at the subject residence. As such, your affiant assesses that critical evidence of a crime will be

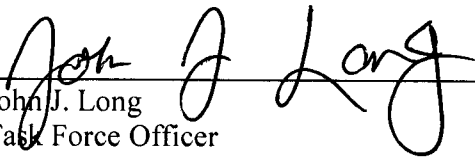
¹⁸ Your affiant is aware that the Arabic term "haram" is used to refer to any act that this forbidden in Islam.

discovered at the location(s) set forth in Attachment A and therefore requests authority to seize the items set forth in Attachment B.

REQUEST FOR SEALING

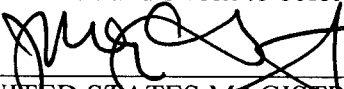
44. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation by causing flight of the targets, destruction of evidence, and other forms of obstruction. I further request that these documents may be shared with other law enforcement personnel, at the discretion of the government and as otherwise required for investigative or national security purposes

Respectfully submitted,



John J. Long
Task Force Officer
Federal Bureau of Investigation

Subscribed and sworn to before me on 19 October, 2015



UNITED STATES MAGISTRATE JUDGE
JAMES E. GATES

ATTACHMENT A

Property to be Searched

The Location of: 205 Duxbury Drive, Raleigh, NC, 27607 is a single home residence in Raleigh, North Carolina. The residence is two stories with a brick front. The front and garage doors are white in color and the black mailbox located in front of the residence, near the road, has the number "205" on it. The residence is located in the Braeloch neighborhood on Duxbury Drive, in between Fincastle Drive and McCleary Court. Areas to be searched specifically include any common areas of the residence accessible by ABU-HAMMAD (e.g., kitchen, living room, family room, etc.) and any personal space he may possess (e.g, his designated room and/or sleeping space); areas explicitly excluded include the room(s) and/or exclusive personal space(s) used solely by ABU-HAMMAD's parents and/or brothers unless there is indication that ABU-HAMMAD has access to and uses any computer media in such areas or stores any personal property in such areas.

The Person of: Ameer Abu-Hammad

The Items of: The computer(s), laptops, cellular phones, and all other electronic devices capable of communication via the internet as well as any form of electronic device potentially capable of containing records, documents, or materials as described in affidavit utilized by Ameer Abu-Hammad in support for terrorism and/or violence.

ATTACHMENT B

PROPERTY TO BE SEARCHED AND/OR SEIZED

This warrant authorizes (i) the search of the property identified in Attachment A for only the following and (ii) authorizes the seizure of the items listed below only to the extent they constitute the following:

- (a) Evidence of violations of Title 18, United States Code, Section 2339B (“subject violation”); or
- (b) Any item constituting contraband due to the subject violations, fruits of the subject violations, or other items possessed whose possession is illegal due to the subject violations; or
- (c) Any property designed for use, intended for use, or used in committing any subject violations.

Subject to the foregoing, the items authorized to be seized include the following:

- 1. Computers, cellular telephones, and electronic devices capable of communication via the internet as well as any form of electronic device potentially capable of containing records, documents, or materials indicating:
 - a. Support for terrorism and/or violence;
 - b. International travel;
 - c. Ownership or use of the device(s)
 - d. Occupancy and/or residency at the subject premises.
- 2. Any physical record, document, or material indicating
 - a. Support for terrorism and/or violence;
 - b. International travel;
 - c. Ownership or use of the device(s) described in #1 above;
 - d. Occupancy and/or residency at the subject premises.



ATTACHMENT C

COMPUTER SEARCH PROTOCOL

1. Definition of "Computer." Unless otherwise defined in the warrant, "computer" means any electronic, magnetic, optical, electro-chemical, or other data processing device performing logical or storage functions, and includes any information storage facility, communications facility, or other equipment or media directly related to or operating in conjunction with such device. "Computer" also includes the system software (*e.g.*, operating systems, interfaces, hardware drivers), applications software, and related instruction manuals or other documentation and data security devices (*e.g.*, passwords, keycards) needed to conduct the search authorized by the warrant. "Media" as used in this definition means all forms of material or devices that are capable of storing or preserving electronic information (*i.e.*, data of any kind).

2. On-Site Search. To the extent practicable, the computer described in the warrant shall be analyzed at the search site (*i.e.*, the location identified in the warrant) and not seized for analysis off-site. Alternatives to seizure for purposes of analysis off-site that may be considered by the government include, but are not limited to, the following:

- a. identification of a knowledgeable person at the search site who could assist the government in locating information subject to the warrant;
- b. use by the government of its own expert at the search site to locate the information subject to the warrant;
- c. creation at the search site of an electronic mirror image of those parts of the computer that are likely to contain information subject to the warrant and subsequent analysis of such mirror image copy off-site in lieu of the computer.

3. Seizure for Analysis Off-Site. If any computer subject to the warrant cannot practicably be analyzed at the search site, the warrant allows for seizure of such computer and its removal from the search site to a laboratory, controlled environment, or other off-site location for purposes of analysis. Such off-site analysis shall be completed as promptly as practicable. If upon completion of the off-site analysis the government determines that the computer and the information stored in it are not subject to permanent seizure as contraband (*i.e.*, property used in furtherance of criminal activity), fruits of criminal activity, or on other grounds, the government shall return the computer to the person from whom or from whose premises it was taken. Such return shall be made as soon as practicable after completion of the analysis.

4. Seizure as Contraband or Instrumentality. The government may permanently seize a computer and information stored therein that the government identifies (in connection with either an on-site or off-site search) as contraband, fruits of criminal activity, or otherwise subject to permanent seizure if the warrant allows for such permanent seizure. If the warrant does not authorize such permanent seizure, the government shall obtain another warrant supported by probable cause authorizing permanent seizure before affecting it. If the computer had initially been seized only for purposes of analysis off-site, the government shall notify the issuing Magistrate Judge of its determination to permanently seize the computer and/or information stored therein.

5. Storage of Information on Seized Computer. The government shall make a copy of all information stored on the computer as soon as practicable after the computer's seizure except as otherwise provided by the warrant. Such copy shall not be analyzed by the government except as reasonably necessary to confirm that it is an accurate copy, but shall be retained until further order of the court as a record of the state of the computer and the information therein prior to any subsequent analysis by the government. The government shall not reconfigure the computer until such copy has been made.

6. Return of Information from Seized Computer. If any person from which or from whose premises a computer is seized either for off-site analysis or permanently so requests in writing, the government shall provide to the person within a reasonable time of the request copies of any requested information not subject to permanent seizure (as contraband, fruits of criminal activity, or on other grounds) that may reasonably be necessary or important to the continuing functioning of the person's legitimate activities. If the government withholds any information requested, it shall within a reasonable time of the request identify to the person making the request the information being withheld and the reasons for withholding it.

7. Search Methodology. In conducting the search authorized by this warrant, whether performed on-site or off-site, the government shall make reasonable efforts to utilize a computer search methodology to search for and seize only that information which is identified in the warrant as subject to such search or seizure. The search methodology may include, but is not limited to, the following techniques:

- a. surveying various file "directories" and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files);
- b. "opening" or cursorily reading the first few "pages" of such files in order to determine their precise contents;
- c. "scanning" storage areas to discover and possibly recover recently deleted data;
- d. scanning storage areas for deliberately hidden files; or

- e. performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation.

8. Inventories. When a computer has been seized for analysis off-site, the government shall comply with Fed. R. Crim. P. 41(f) in the following manner:

- a. Initial Inventory. Following the on-site search and seizure, the government shall prepare the usual Rule 41(f) inventory of not only the property and items seized by it pursuant to the warrant, but also the information, which has, at that date, been identified as seized pursuant to the warrant. This inventory shall identify each computer that will be subject to further off-site analysis. For example, if the government makes an on-site mirror image of a computer for use in an off-site analysis, the government need only list the making of the mirror image in the return, with an indication that it is subject to further searching pursuant to this warrant. The listing of any information that is seized from the computer off-site will then be made in the final inventory. The government shall give a copy of the warrant and this initial inventory of property seized to the person from whom or from whose premises the property was taken and make a return to the court, all as provided by Rule 41(f). Because of the nature of electronic or computer information, the listing of seized information in either the initial or final inventory may be made by copying the seized information to a computer diskette, compact disc (*i.e.*, CD), DVD, or like storage device and submitting it along with an affidavit which describes the contents of the storage device.
- b. Final Inventory. After completing the off-site analysis of the computer, the government shall prepare a final inventory of information seized during the off-site analysis. The government shall deliver a copy of the final inventory to the person from whom or from whose premises the computer was taken and make a return of the original final inventory to the court. The court will then attach this final inventory to the original search warrant and initial inventory as an addendum.



ATTACHMENT C

COMPUTER SEARCH PROTOCOL

1. Definition of "Computer." Unless otherwise defined in the warrant, "computer" means any electronic, magnetic, optical, electro-chemical, or other data processing device performing logical or storage functions, and includes any information storage facility, communications facility, or other equipment or media directly related to or operating in conjunction with such device. "Computer" also includes the system software (*e.g.*, operating systems, interfaces, hardware drivers), applications software, and related instruction manuals or other documentation and data security devices (*e.g.*, passwords, keycards) needed to conduct the search authorized by the warrant. "Media" as used in this definition means all forms of material or devices that are capable of storing or preserving electronic information (*i.e.*, data of any kind).
2. On-Site Search. To the extent practicable, the computer described in the warrant shall be analyzed at the search site (*i.e.*, the location identified in the warrant) and not seized for analysis off-site. Alternatives to seizure for purposes of analysis off-site that may be considered by the government include, but are not limited to, the following:
 - a. identification of a knowledgeable person at the search site who could assist the government in locating information subject to the warrant;
 - b. use by the government of its own expert at the search site to locate the information subject to the warrant;
 - c. creation at the search site of an electronic mirror image of those parts of the computer that are likely to contain information subject to the warrant and subsequent analysis of such mirror image copy off-site in lieu of the computer.
3. Seizure for Analysis Off-Site. If any computer subject to the warrant cannot practicably be analyzed at the search site, the warrant allows for seizure of such computer and its removal from the search site to a laboratory, controlled environment, or other off-site location for purposes of analysis. Such off-site analysis shall be completed as promptly as practicable. If upon completion of the off-site analysis the government determines that the computer and the information stored in it are not subject to permanent seizure as contraband (*i.e.*, property used in furtherance of criminal activity), fruits of criminal activity, or on other grounds, the government shall return the computer to the person from whom or from whose premises it was taken. Such return shall be made as soon as practicable after completion of the analysis.

4. Seizure as Contraband or Instrumentality. The government may permanently seize a computer and information stored therein that the government identifies (in connection with either an on-site or off-site search) as contraband, fruits of criminal activity, or otherwise subject to permanent seizure if the warrant allows for such permanent seizure. If the warrant does not authorize such permanent seizure, the government shall obtain another warrant supported by probable cause authorizing permanent seizure before affecting it. If the computer had initially been seized only for purposes of analysis off-site, the government shall notify the issuing Magistrate Judge of its determination to permanently seize the computer and/or information stored therein.

5. Storage of Information on Seized Computer. The government shall make a copy of all information stored on the computer as soon as practicable after the computer's seizure except as otherwise provided by the warrant. Such copy shall not be analyzed by the government except as reasonably necessary to confirm that it is an accurate copy, but shall be retained until further order of the court as a record of the state of the computer and the information therein prior to any subsequent analysis by the government. The government shall not reconfigure the computer until such copy has been made.

6. Return of Information from Seized Computer. If any person from which or from whose premises a computer is seized either for off-site analysis or permanently so requests in writing, the government shall provide to the person within a reasonable time of the request copies of any requested information not subject to permanent seizure (as contraband, fruits of criminal activity, or on other grounds) that may reasonably be necessary or important to the continuing functioning of the person's legitimate activities. If the government withholds any information requested, it shall within a reasonable time of the request identify to the person making the request the information being withheld and the reasons for withholding it.

7. Search Methodology. In conducting the search authorized by this warrant, whether performed on-site or off-site, the government shall make reasonable efforts to utilize a computer search methodology to search for and seize only that information which is identified in the warrant as subject to such search or seizure. The search methodology may include, but is not limited to, the following techniques:

- a. surveying various file "directories" and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files);
- b. "opening" or cursorily reading the first few "pages" of such files in order to determine their precise contents;
- c. "scanning" storage areas to discover and possibly recover recently deleted data;
- d. scanning storage areas for deliberately hidden files; or

- e. performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation.

8. Inventories. When a computer has been seized for analysis off-site, the government shall comply with Fed. R. Crim. P. 41(f) in the following manner:

- a. Initial Inventory. Following the on-site search and seizure, the government shall prepare the usual Rule 41(f) inventory of not only the property and items seized by it pursuant to the warrant, but also the information, which has, at that date, been identified as seized pursuant to the warrant. This inventory shall identify each computer that will be subject to further off-site analysis. For example, if the government makes an on-site mirror image of a computer for use in an off-site analysis, the government need only list the making of the mirror image in the return, with an indication that it is subject to further searching pursuant to this warrant. The listing of any information that is seized from the computer off-site will then be made in the final inventory. The government shall give a copy of the warrant and this initial inventory of property seized to the person from whom or from whose premises the property was taken and make a return to the court, all as provided by Rule 41(f). Because of the nature of electronic or computer information, the listing of seized information in either the initial or final inventory may be made by copying the seized information to a computer diskette, compact disc (*i.e.*, CD), DVD, or like storage device and submitting it along with an affidavit which describes the contents of the storage device.
- b. Final Inventory. After completing the off-site analysis of the computer, the government shall prepare a final inventory of information seized during the off-site analysis. The government shall deliver a copy of the final inventory to the person from whom or from whose premises the computer was taken and make a return of the original final inventory to the court. The court will then attach this final inventory to the original search warrant and initial inventory as an addendum.